ANÁLISIS DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN EN LA VEEDURÍA DISTRITAL CON ENFASIS EN DIRECTORIO ACTIVO

ERIC JOHANN BAQUERO PARDO

FABIO NELSON FRANCO HERNANDEZ

Trabajo de Grado presentado para optar al título de Especialista en Seguridad de la Información

Asesor: Hector Dario Jaimes Parada, Magíster (MSc) en Seguridad Informática

Universidad Católica de Colombia

Facultad de Ingeniería

Especialización en Seguridad de la Información

Bogotá D.C., Colombia

2019

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

La información hoy en día es uno de los activos más importantes con los que cuenta la Veeduría Distrital, sin embargo, no siempre tiene la consideración e importancia necesaria dentro de la organización.

La Veeduría Distrital es un órgano de control preventivo de Bogotá que contribuye a mejorar la gestión de las entidades distritales, a cualificar a más ciudadanía para el cuidado de lo público y a que se tomen las mejores decisiones con base en argumentos técnicos y en procesos transparentes.

Es necesario hacer ver a la Veeduría Distrital la importancia que tiene la seguridad de su información almacenada en los recursos compartidos a la cual se tiene acceso con los usuarios creados en el Directorio Activo.

El proyecto que se realizará ha sido denominado "ANALISIS DE GESTION DE LA SEGURIDAD DE LA INFORMACION EN LA VEEDURIA DISTRITAL CON ENFASIS EN EL DIRECTORIO ACTIVO", el cual está basado en las mejores prácticas y estándares internacionales como ISO 270001.

Como resultado de este análisis se entregará a la Veeduría un informe con las recomendaciones que le garanticen la confidencialidad, integridad y disponibilidad de la información que se maneja al interior de la entidad y que a la vez se inicie una cultura de buenas prácticas sobre la configuración y gestión del directorio activo que actualmente se tiene implementado.

1 GENERALIDADES

Intro

1.1 LÍNEA DE INVESTIGACIÓN

Gestión Integral y dinámica de las Organizaciones Empresariales

1.2 PLANTEAMIENTO DEL PROBLEMA

Actualmente el riesgo de fraude dentro de una organización es una amenaza que involucra a los diferentes niveles jerárquicos que la conforman, y la materialización de este tipo de riesgo tiene consecuencias tanto económicas como de reputación que afectarían el sector distrital.

En la Veeduría Distrital se busca salvaguardar la información, por esta razón se pretende realizar un análisis de vulnerabilidades, detectando las posibles fallas que presenta el directorio activo que tiene la entidad, ya que es de conocimiento de los autores, que en los últimos 5 años no se ha realizado un análisis de vulnerabilidades al Directorio Activo, como tampoco se han actualizado los protocolos de gestión de la seguridad para el mismo.

Se hace evidente la necesidad, no solo de realizar un análisis de vulnerabilidades con recomendaciones al directorio activo, sino también una evaluación de la gobernabilidad de la seguridad de la información, teniendo como base la norma ISO 27001 en lo referente al control de accesos, sección A.9.1.2 y A.11 del Anexo A, enmarcadas dentro de la ejecución de funciones establecidas, para lograr que la información este salvaguardada en la entidad.

1.2.1 Antecedentes del problema

La Veeduría Distrital es el órgano de control preventivo de la ciudad de Bogotá, cuya función principal es prevenir posibles actos de corrupción en las entidades del distrito, con información susceptible como son las denuncias e investigaciones que realiza la ciudadanía. Así mismo, la Veeduría cuenta con un grupo de investigación que realiza indagaciones a las diferentes entidades distritales, por lo cual, la información que se maneja es de carácter confidencial. [QRI-CP-01] Caracterización del Proceso Gestión e Investigación de Quejas y Reclamos en el Distrito Capital - V2

Respecto al problema a tratar, se tiene que la implementación del directorio activo se realizó en el año 1997 con un servidor Windows NT, ya que se contaba con una infraestructura pequeña y suplía las necesidades de la entidad. Ya en el año 2008 se realizó la compra de un servidor con sistema operativo Windows 2003, y de esta forma se fueron creando en él todas las dependencias y usuarios que laboran en la entidad, el cual se ha mantenido hasta la fecha.

Por las condiciones culturales de la organización no se ha permitido realizar procesos de detección de vulnerabilidades y de esta forma propender por salvaguardar la información, pero a pesar de lo anterior, afortunadamente no se ha evidenciado ningún impacto negativo dentro de la Veeduría Distrital.

También se detecta que en los últimos cinco años no se ha contratado ningún servicio especializado para que realice recomendaciones al directorio activo de la Veeduría Distrital, y adicionalmente, no se cuenta con un procedimiento claro en seguridad de la información, que sea difundido periódicamente con carácter obligatorio, por ende su aplicación y actualización es nula.

Referente a la confidencialidad de la información, se observa que los usuarios se pueden llevar la información, debido a que los permisos que se tienen otorgados desde el directorio activo así lo permiten. Desde el punto de vista de la disponibilidad, en caso de un ataque por

malware tipo ransomware o similar, se podría perder el registro de los usuarios y sus perfiles de seguridad, ya que no se tiene un respaldo o backup del directorio activo, según lo verificado en la entidad.

1.2.2 Pregunta de investigación

¿Cuenta la Veeduría Distrital con una adecuada gestión de la seguridad de la información enfocada al control de acceso, seguridad de las redes y gestión de vulnerabilidades del directorio activo implementado en la actualidad?

Variables del problema

- Procedimientos para llevar el registro de los usuarios que se crean modifican o eliminan en la entidad.
- Procedimientos de análisis de vulnerabilidades a la plataforma informática.
- Servidores
- Sistemas operativos con sus políticas de parcheo y cambio de versiones por finalización de soporte por parte del fabricante.
- El directorio activo
- Usuarios y permisos a carpetas compartidas.
- Información no estructurada

1.2.3 Factores Críticos de Éxito del Proyecto

- Que se tenga el acta de aceptación del proyecto firmada por Veeduría Distrital.
- Que en el análisis de la gestión de la Seguridad de la información se encuentren oportunidades de mejora.
- Que en el análisis de vulnerabilidades al directorio Activo se encuentren hallazgos que permitan generar recomendaciones.

1.3 JUSTIFICACIÓN

Se vislumbra que la Veeduría Distrital cuenta con un sistema de gestión de la seguridad de la información que es susceptible de actualización y mejoras frene a referentes internacionales, enfatizando en la gestión del Directorio Activo. El análisis que vamos a desarrollar tendrá un impacto en la sociedad ya que las recomendaciones resultado de este trabajo, orientarán a la entidad a que la información propia y la de los ciudadanos, cumpla con los parámetros mínimos de confidencialidad, integridad y disponibilidad.

Al implementar en la entidad las recomendaciones dadas como resultado de este proyecto se fortalecerá el nivel de seguridad de la información en la entidad y por ende generará confianza en la ciudadanía para tener mayor contacto con los entes de vigilancia y control a nivel distrital

Y desde el punto de vista de los autores, también se justifica este proyecto con el fin de fortalecer los conocimientos adquiridos en la especialización y aplicarlos con suficiencia y pertinencia en el sector distrital.

1.4 OBJETIVOS

1.4.1 Objetivo general

Hacer un análisis del Directorio Activo en la Veeduría Distrital y evaluar la gobernabilidad de la seguridad de la Información al interior de la entidad en lo referente a las políticas de control de accesos, seguridad de las redes y gestión de vulnerabilidades del directorio activo.

1.4.2 Objetivos específicos

- Informar del estado actual de la seguridad Información en la Veeduría Distrital.
- Generar las recomendaciones respecto al directorio activo, tomando como criterios la norma ISO27001:2013 y 27002:2013 anexos A.9 Control de accesos, A.13 Seguridad de las comunicaciones y A.12.6.1 Gestión de las vulnerabilidades técnicas, en concordancia con los hallazgos obtenidos.
- Realizar una prueba piloto de remediación de vulnerabilidades del Directorio Activo

- Incluir en el informe final las oportunidades de mejora en la gestión de la seguridad de la información enfocada al directorio activo en la Veeduría Distrital.

1.5 CRONOGRAMA

EDT	Nombre de tarea	Duración	Comienzo	Fin
1.1	**reuniones**	**91,25 días**	**mié 27/03/19**	**lun 12/08/19**
1.1.1	**Reunion con el Tutor**	**42,13 días**	**mié 27/03/19**	**mié 29/05/19**
1.1.1.1	Reunion con el Tutor 1	1 hora	mié 27/03/19	mié 27/03/19
1.1.1.2	Reunion con el Tutor 2	1 hora	mié 3/04/19	mié 3/04/19
1.1.1.3	Reunion con el Tutor 3	1 hora	mié 10/04/19	mié 10/04/19
1.1.1.4	Reunion con el Tutor 4	1 hora	mié 17/04/19	mié 17/04/19
1.1.1.5	Reunion con el Tutor 5	1 hora	mié 24/04/19	mié 24/04/19
1.1.1.6	Reunion con el Tutor 6	1 hora	jue 2/05/19	jue 2/05/19
1.1.1.7	Reunion con el Tutor 7	1 hora	mié 8/05/19	mié 8/05/19
1.1.1.8	Reunion con el Tutor 8	1 hora	mié 15/05/19	mié 15/05/19
1.1.1.9	Reunion con el Tutor 9	1 hora	mié 22/05/19	mié 22/05/19
1.1.1.10	Reunion con el Tutor 10	1 hora	mié 29/05/19	mié 29/05/19
1.1.2	**Reuniones con la Veeduria**	**86,25 días**	**mié 3/04/19**	**lun 12/08/19**
1.1.2.1	Reunion 1	2 horas	mié 3/04/19	mié 3/04/19
1.1.2.2	Reunion 2	2 horas	lun 12/08/19	lun 12/08/19
1.2	Gestion	1 día	jue 4/04/19	jue 4/04/19
1.3	Analisis del entorno	1 día?	vie 5/04/19	vie 5/04/19

EDT	Nombre de tarea	Duración	Comienzo	Fin
2	**Estado actual del DA de la veeduria**	**5 días**	**lun 22/07/19**	**vie 26/07/19**
2.1	Levantar informacion del DA	5 días	lun 22/07/19	vie 26/07/19
3	**Analisis de vulnerabilidades DA Veeduria Distrital**	**7 días**	**lun 29/07/19**	**mar 6/08/19**
3.1	**Planificar el Ataque**	**3 días**	**lun 29/07/19**	**mié 31/07/19**
3.1.1	Definir el Ataque	1 día	lun 29/07/19	lun 29/07/19
3.1.2	Definir las herramientas	1 día	mar 30/07/19	mar 30/07/19
3.1.3	Definir el presupuesto	1 día	mié 31/07/19	mié 31/07/19
3.2	**Especificar el Ataque**	**2 días**	**jue 1/08/19**	**vie 2/08/19**
3.2.1	Realizar Ataque Herramienta 1	1 día	jue 1/08/19	jue 1/08/19
3.2.2	Realizar Ataque Herramienta 2	1 día	vie 2/08/19	vie 2/08/19
3.3	**Resultados del Ataque**	**2 días**	**lun 5/08/19**	**mar 6/08/19**
3.3.1	Elaborar el resultado del Ataque 1	1 día	lun 5/08/19	lun 5/08/19
3.3.2	Elaborar el resultado del Ataque 2	1 día	mar 6/08/19	mar 6/08/19

EDT	Nombre de tarea	Duración	Comienzo	Fin
4	**Analisis de los documentos asociados a la seguridad de la informacino del DA**	**6,67 días**	**jue 8/08/19**	**vie 16/08/19**
4.1	Levantar informacion de los procedimientos, politicas, normas, etc., publicados en los cuales interventa asignacion por directorio activo	6,67 días	jue 8/08/19	vie 16/08/19

EDT	Nombre de tarea	Duración	Comienzo	Fin
5	**Informe de vulnerabilidades en el DA de la Veeduria Distrtal**	**55 días**	**vie 16/08/19**	**mié 6/11/19**
5.1	Analizar el resultado de los ataques 1 y 2	30 días	vie 16/08/19	lun 30/09/19
5.2	Analizar la informacion obtenida para generar recomendaciones documentales DA	15 días	lun 30/09/19	mar 22/10/19
5.3	Documentar las recomendaciones DA	5 días	mar 22/10/19	mar 29/10/19
5.4	Documentar las recomendaciones de los procedimientos, politicas normas, etc. aplicables al DA	5 días	mar 29/10/19	mié 6/11/19
6	**Trabajo de Grado**	**112,13 días**	**vie 31/05/19**	**vie 15/11/19**
6.1	Sustentacion del anteproyecto	1 hora	vie 31/05/19	vie 31/05/19
6.2	Sustentacion Proyecto	1 hora	vie 15/11/19	vie 15/11/19

1.6 PRESUPUESTO

En las siguientes tablas se encuentra detallado el presupuesto estimado para el desarrollo del proyecto.

Tabla 1-1. Presupuesto global de la propuesta por fuentes de financiación (en miles de $).

RUBROS	VALOR UNITARIO	VALOR TOTAL
PERSONAL	Ver tabla 1-2	60.000
EQUIPOS	Var tabla 1-4	1.400
SOFTWARE	0	0
MATERIALES	Ver tabla 1-8	100
SALIDAS DE CAMPO	4	120
MATERIAL BIBLIOGRÁFICO	70	70
PUBLICACIONES Y PATENTES	0	0
SERVICIOS TÉCNICOS	0	0
VIAJES	0	0
CONSTRUCCIONES	0	0
MANTENIMIENTO	0	0
ADMINISTRACION	0	0
TOTAL	61.690	61.690

Tabla 1-2. Descripción de los gastos de personal (en miles de $).

INVESTIGADOR / EXPERTO/ AUXILIAR	FORMACIÓN ACADÉMICA	FUNCIÓN DENTRO DEL PROYECTO	DEDICACIÓN Horas/semana	VALOR
Eric Baquero	Ing. Sistemas		20	1.000 semana
Fabio			20	1.000 semana
TOTAL (30 semanas)				**60.000**

Tabla 1-3. Descripción de los equipos que se planea adquirir (en miles de $).

EQUIPO	JUSTIFICACIÓN	VALOR TOTAL
N/A		
TOTAL		

Tabla 1-4. Descripción y cuantificación de los equipos de uso propio (en miles de $)

EQUIPO	VALOR TOTAL
2 PC Portátil (10 meses) Valor equipo $2.000.000	1.400
TOTAL	1.400

Tabla 1-5. Descripción del software que se planea adquirir (en miles de $).

SOFTWARE	JUSTIFICACIÓN	VALOR TOTAL
N/A		
TOTAL		

Tabla 1-6. Descripción y justificación de los viajes (en miles de $).

LUGAR / NO. DE VIAJES	JUSTIFICACIÓN[1]	PASAJES ($)	ESTADÍA ($)	TOTAL DÍAS	TOTAL
N/A					

[1] Se debe justificar cada viaje en términos de su necesidad para el éxito del proyecto

TOTAL					

Tabla 1-7. Valoración de las salidas de campo (en miles de $).

ITEM	COSTO UNITARIO	#	TOTAL
Visita Veeduría	30	4	120
TOTAL			120

Tabla 1-8. Materiales y suministros (en miles de $)

MATERIALES[2]	JUSTIFICACIÓN	VALOR TOTAL
Papelería	Informes	100
TOTAL		100

Tabla 1-9. Bibliografía (en miles de $).

ÍTEM	JUSTIFICACIÓN	VALOR TOTAL
Norma ISO 27001		70
TOTAL		70

Tabla 1-10. Servicios Técnicos (en miles de $).

TIPO DE SERVICIOS	JUSTIFICACIÓN	VALOR TOTAL
N/A		
TOTAL		

Nota: Formato utilizado por Colciencias.

[2] Pueden agruparse por categorías, ej: vidriería, reactivos, papelería, suscripciones a revistas, libros, etc.

2 MARCOS DE REFERENCIA

2.1 MARCO CONCEPTUAL

En el año 2000 Microsoft realiza una innovación con el desarrollo del Directorio Activo ya que la idea tampoco fue directamente de Microsoft si no que fue una implantación mejorada del servicio de Directorio de Novell el cual aparece en el año 1983 para ejecutarse en un servidor basado en el microprocesador Motorola MC68000 usando configuración de red Novell S-Net.

En este punto de la historia, es cuando ya es necesario abandonar definitivamente los desarrollos en 16 bits y plantearse seriamente la integración en un único sistema operativo. Las tecnologías básicas ya estaban probadas y funcionando, por lo que Microsoft se embarcó en el proyecto que originalmente fue llamado Whistler que desemboco en la serie de los núcleos de XP y la serie .NET lo cual permitió la evolución del Windows 2000 Server, Advanced Server y Datacenter, en cuatro versiones .NET: Server Web, Standard Web, Enterprise Web y Datacenter.

Windows 2000 es un sistema operativo de Microsoft que se puso en circulación el 17 de febrero de 2000 con un cambio de nomenclatura para su sistema NT. Así, Windows NT 5.0 pasó a llamarse Windows 2000. Fue sucedido por Windows XP para equipos de escritorio en octubre de 2001 y Windows Server 2003 para servidores en abril de 2003.

Todo esto con el fin de obtener un directorio activo interoperable con otros servicios de directorio. Entre estos estándares, podemos destacar los siguientes:

- DCHP: (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de ordenadores, que permite la administración desatendida de características de red.
- DNS: (Domain Name System). Servicio de nombres de dominio que permite la

administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.

- SNTP: (Simple Network Time Protocol). Protocolo simple de tiempo de red, que permite disponer de un servicio de sincronización de tiempo entre sistemas conectados por red.

- LDAP: (Lightweight Directory Access Protocol). Protocolo ligero (o compacto) de acceso a directorio. Este es el protocolo mediante el cual las aplicaciones acceden para leer o modificar la información existente en la base de datos del directorio.
- KERBEROS: Protocolo utilizado para la autenticación de usuarios y máquinas.

- CERTIFICADO X.509 Estándar que permite distribuir información a través de la red de una forma segura.

2.2 ESTADO DEL ARTE:

Actualmente para las entidades tanto distritales como de nación se tienen establecidos mecanismos orientados a la seguridad de la información. Para el desarrollo de este proyecto se definió lo siguiente:

A nivel de la Veeduría Distrital se tiene un modelo de seguridad y privacidad de la información. Mediante Resolución 166 del 10/08/2017, se adopta la Política de Seguridad de la Información de la Veeduría Distrital.
http://veeduriadistrital.gov.co/sites/default/files/files/RESOLUCION%20166%20DE%202017%20POLITICA%20DE%20SEGURIDAD%20DE%20INFO.pdf

Como lo describe el Documento CONPES 3854 en su política nacional de seguridad digital, se evidencia un aumento significativo en la participación digital de los ciudadanos, lo que a su vez se traduce en una economía digital con cada vez más participantes en el país.
Desafortunadamente, el incremento en la participación digital de los ciudadanos, trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado.

Para lograr fortalecer esto el CONPES trae una definición de política con el fin de implementar la política nacional de seguridad digital.

En los artículos que se mencionan a continuación se observan diferentes problemáticas tratadas en el directorio activo:

F.J. Quevedo Armijos, J.E. Sesme Candelario, "Análisis de Vulnerabilidades en los Servicios ACTIVE DIRECTORY, DNS y DHCP Instalados en los Sistemas Operativos Windows Server (2008, 2012, 2016) Utilizando Herramientas de Test de Intrusión.", tesis, Univ. De Guayaquil, 2018 [En línea]. Disponible en: http://repositorio.ug.edu.ec/handle/redug/27022 [Accedido: 28-May-2019]. Nos muestra cómo se pueden realizar intrusiones atreves del DNS y el DHCP.

J.C. Bermeo Oyola, "IMPLEMENTACIÓN DE HACKING ÉTICO PARA LA DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES DE RED EN LA EMPRESA COMPLEX DEL PERÚ S.A.C.-TUMBES; 2017.", tesis maestría, Univ. Católica Los Ángeles Chimbote, 2017 [En línea]. Disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/10386/IMPLEMENTACION_SEGURIDAD_INFORM%c3%81TICA_BERMEO_OYOLA_JEAN_CARLOS.pdf?sequence=1&isAllowed=y [Accedido: 28-May-2019]. En este documento se muestran los riesgos de cómo se encuentra una red y cómo se pueden detectar sus posibles vulnerabilidades. Bermeo Oyola, Jean Carlos (2019)

D.E. Ojeda Pereira, M.M Muñoz, "Análisis de las vulnerabilidades en el manejo de la información bajo la norma ISO/IEC 27001:2013, en la empresa Gestión & Negocios Administrativos SAS del Distrito de Riohacha – La Guajira", Monografía, Univ. UNAD, 2018 [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/24501 [Accedido: 28-May-2019]. Como se utiliza la norma ISO 27001:2013.

A.J. Llanos Ruiz, M.A. Meneses Ortiz, "Diseño de un protocolo para la detección de

vulnerabilidades en los principales servidores de la Superintendencia de Puertos y Transporte", tesis, Univ, Católica de Colombia Sede Bogotá, 2016 [En línea]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/14013/4/Proyecto%20de%20Grado.pdf [Accedido: 28-May-2019].Después de una investigación a nivel nacional no se encontró documentación pública de trabajos de investigación en el área de estudio de este proyecto, solo lo mencionado en párrafos anteriores.

3 METODOLOGÍA

Para el desarrollo de este proyecto se plantea la ejecución por fases como se muestra a continuación en el diccionario de datos de la EDT (Estructura de Desglose del Trabajo).

3.1 DICCIONARIO DE DATOS DE LA EDT

Tabla 3.1 Diccionario de Datos EDT

PROYECTO: Análisis de gestión de la seguridad de la información en la veeduría distrital con énfasis en directorio activo.
ID del paquete de trabajo: 1.0
Definición: **Gerencia del proyectos**
Descripción: Reuniones, gestión y análisis del entorno de la Veeduría Distrital.
ID del paquete de trabajo: 2.0
Definición: **Evaluación del Estado actual del directorio activo**
Descripción: Levantar información del directorio activo.
ID del paquete de trabajo: 3.0
Definición: **Análisis de vulnerabilidades en el directorio activo**
Descripción: Planificar el ataque, definir las herramientas, definir el presupuesto, especificar el ataque, especificar las herramientas, resultado del ataque
ID del paquete de trabajo: 4.0
Definición: **Informe de vulnerabilidades en el Directorio Activo**
Descripción: Analizar el resultado del ataque 1 y 2
ID del paquete de trabajo: 5.0
Definición: **Trabajo de grado**
Descripción**:** Sustentación del anteproyecto

ASIGNACIÓN A INGENIEROS: Fabio Franco, Eric Baquero	
Fecha: Asignada: 08/03/2019	Fecha de Entrega: 07/06/2019
Costo Estimado: M$ 61.690	

3.2 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Software libre

- Nessus: para observar las vulnerabilidades que se tienen en los servidores de la entidad.
- Nmap: para identificar los puertos a los cuales se realizará el ataque.
- Metaexploit: para poder ejecutar las vulnerabilidades que se detecten en el Directorio Activo.

Documentación de Microsoft (MS)

- Planeación y diseño de AD DS
- Procedimientos recomendados para proteger Active Directory
- Protección de los controladores de dominio frente a ataques
- Reducción de la superficie de ataque de Active Directory
- Planeación y diseño de AD DS

La Normas

- ISO27001, sección A.9.1.2 y A.11 del Anexo A.
- ISO 27002 sección A.9.1.2 y A.11 del Anexo A

3.3 POBLACIÓN Y MUESTRA

La población objeto de estudio del presente proyecto está conformada por los funcionarios y contratistas de la Veeduría Distrital que actualmente cuenta, como se muestra en la siguiente tabla.

Tabla 3.2 Funcionarios de la Veeduría

FUNCIONARIOS DE LA VEEDURIA DISTRITAL		
Siglas	**Definición**	**Personal**
dpc	Despacho Veedor	10
vic	Viceveeduria	7
cnt	Contabilidad	4
pre	Presupuesto	2
ged	Gestión Documental	7
tah	Talento Humano	10
urc	Gestión Tic	9
ujd	Oficina Asesora Jurídica	11
pln	Oficina Asesora Planeación	10
uci	Oficina Asesora de Control Interno	5
cad	Delegada para la contratación	18
qyr	Delegada para la atención de quejas y reclamos	30
ead	Delegada para la Eficiencia Administrativa y Presupuestal	12
Pcd	Delegada para la Participación Ciudadana	25
trp	Equipo de Transparencia	8
lab	Equipo de Laboratorio	7
eri	Equipo de Relaciones Interinstitucionales.	5
pyc	Prensa y Comunicaciones	8
bys	Bienes y Servicios	16
atc	Atención al ciudadano	3

Dentro de la población está también el parque informático que se compone de 195 equipos de mesa, 8 impresoras y 12 equipos servidores.

La muestra estará conformada por el 5% de los usuarios de cada división, y a nivel de hardware, se tomarán los 4 servidores que contienen los dominios y 1 equipo servidor de archivos.

3.4 Alcances y limitaciones

- El proyecto cubre el análisis del Directorio Activo de la Veeduría Distrital.
- Se realizarán solo las pruebas establecidas en el diccionario de datos, paquete ID 3.0
- Se entregará un informe de evaluación del Directorio Activo.
- Se entregarán las recomendaciones pertinentes para la gestión de la seguridad del

Directorio Activo.

- No se incluyen otro tipo de análisis, evaluaciones, diagnósticos, implementaciones, correcciones en vivo de los hallazgos, elaboración de procedimientos, políticas, ni nada que no esté especificado en el alcance o en el diccionario de datos de la EDT.

Limitaciones: Dentro del presupuesto se estimaron inversiones de M$60. Respecto al tiempo de ejecución de este proyecto, según cronograma, estará enmarcado en 30 semanas. Finalmente, se cuenta con el apoyo del Viceveedor, sin embargo se contemplan limitaciones de tiempo por parte de la disponibilidad de usuarios y equipos objeto del análisis.

El análisis está limitado a los equipos servidores, y usuarios que se definieron en la muestra. (Ver numeral 3.3)

4 PRODUCTOS A ENTREGAR

Informe final que documenta todos los resultados del proyecto, incluyendo los hallazgos, remediaciones y mejores prácticas que se pueden aplicar al Directorio Activo.

Documento con la evaluación de la seguridad de la información aplicable a los controles de acceso con las cuentas de usuario del directorio activo según lo especificado en la norma internacional ISO 27001.

5 RESULTADOS ESPERADOS E IMPACTOS

- Se espera que se pueda realizar el proyecto dentro de las restricciones de tiempo, costo y alcance.
- Que en los análisis realizados se encuentren hallazgos y oportunidades de mejora
- Que se cuente con la colaboración del personal en los procesos de estudio y análisis
- Que las posibles recomendaciones incrementen el nivel de seguridad de la información enfocado al Directorio Activo de la entidad.

En conclusión, que los resultados de este proyecto fortalezcan la gestión de la seguridad de la información de la Veeduría Distrital con enfoque en su Directorio Activo.

Se espera también que en una segunda fase se implementen las recomendaciones sugeridas como resultado de este proyecto, y sean incluidas en los procedimientos del área de tecnología de la Veeduría Distrital.

6 ESTRATEGIAS DE COMUNICACIÓN

Para el desarrollo del proyecto se coordinarán reuniones con el Viceveedor y con el jefe de gestión TIC, para definir la entrega del análisis realizado en el proyecto.

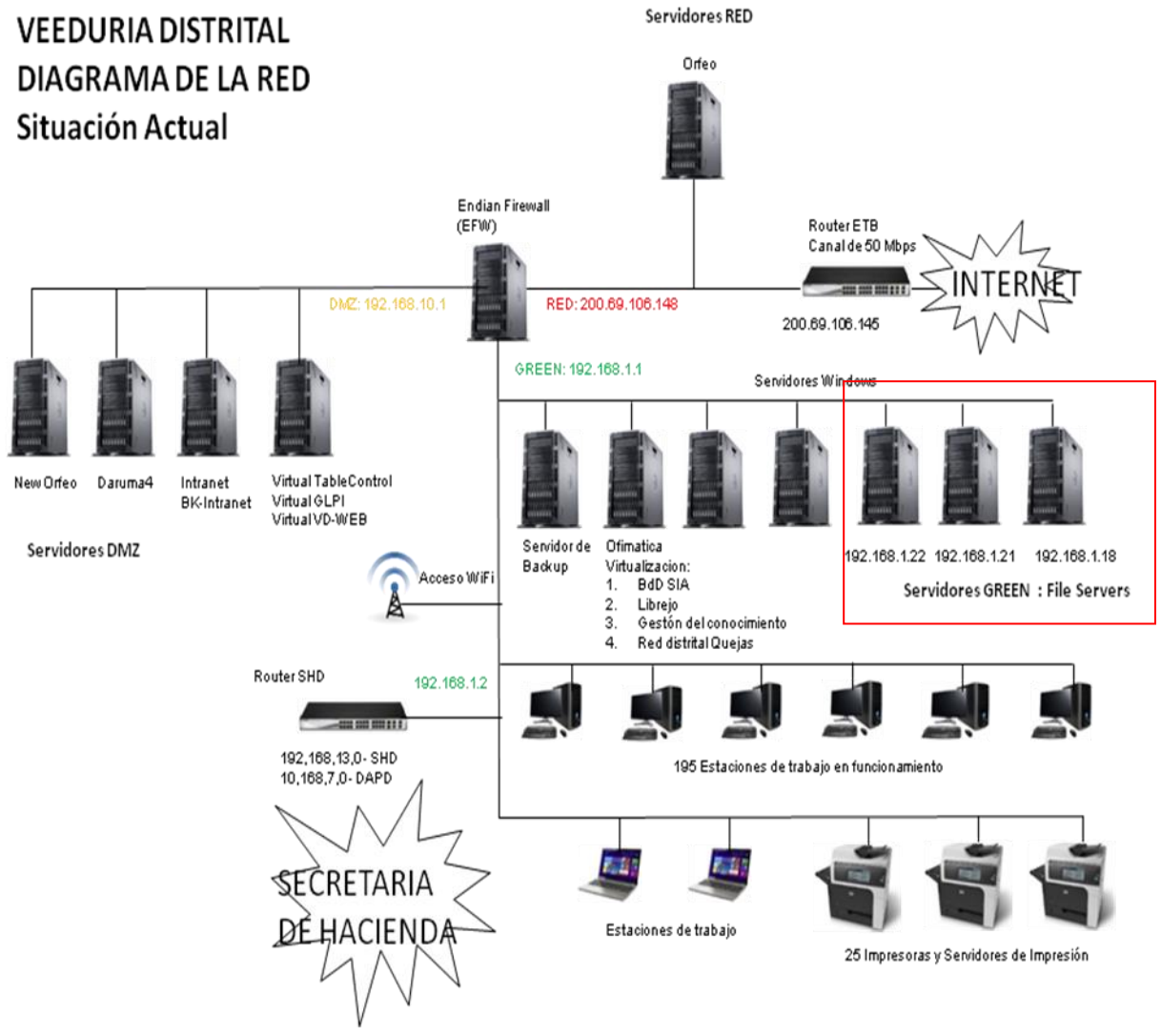
Se realizarán reuniones de seguimiento e información del avance del proyecto cada mes.

Al finalizar el proyecto se realizará una reunión gerencial con las personas que asigne la veeduría distrital para divulgar los hallazgos, las remediaciones y las oportunidades de mejora resultado de la ejecución del proyecto.

7. Desarrollo Del Proyecto

7.1 Levantamiento del estado actual de Directorio Activo de la Entidad

Dentro del levantamiento de información realizado al estado actual del Directorio Activo de la entidad se encontraron que los siguientes servidores soportan los diferentes dominios configurados



Fuente Eric Baquero Imagen 1

Como se observa en el diagrama anterior se cuenta con tres servidores de directorio activo los cuales cuenta con las siguientes especificaciones.

El servidor de 1

Fuente Eric Baquero Imagen 2

El servidor 2

Fuente Eric Baquero Imagen 3

El servidor 3

Fuente Eric Baquero Imagen 4

Una vez identificamos los tres servidores procedimos a la ejecución de las herramientas NMAP y nessus teniendo como resultado:

Servidor 1 se ejecutó el comando nmap –sP dando como resultado 39 equipos con su respectiva MAC Address, ip y tiempo de conexión o latencia.

Adicionalmente se corrió el comando nmap –p 80 y se detecta que los puertos que se encuentran abiertos son 26, entre los que se encuentra el 389 el cual hace referencia al LDAP.

También se ejecutó el programa Nessus el cual detecto las siguientes vulnerabilidades sobre el servidor.

4 criticas
1 alta
5 medias
97 informativas

En estado critican se encuentran

1. Microsoft Windows SMBv1 Multiple Vulnerabilities
2. Unsupported Windows OS (remote)
3. Microsoft IIS 6.0 Unsupported Version Detection

4. Microsoft Windows Server 2003 Unsupported Installation Detection

En estado alto se encuentran

1. MS11-035: Vulnerability in WINS Could Allow Remote Code Execution

En estado medio se encuentran

1. Microsoft Windows SMB LsaQueryInformationPolicy Function SID
2. MS16-047: Security Update for SAM and LSAD Remote
3. Microsoft Windows SMB NULL Session Authentication
4. DNS Server Cache Snooping Remote Information Disclosure

Para mayor información ver anexo informe ejecutivo.

Servidor 2 se ejecutó el comando nmap –sP dando como resultado 106 equipos con su respectiva MAC Address, ip y tiempo de conexión o latencia.

Adicionalmente se corrió el comando nmap –p 80 y se detecta que los puertos que se encuentran abiertos son 32, entre los que se también encuentra el 389 el cual hace referencia al LDAP.

Además, se ejecutó el programa Nessus el cual detecto las siguientes vulnerabilidades sobre el servidor.

14 criticas
12 alta
2 medias
2 baja
120 informativas

En estado crítica se encuentran:

1. Microsoft IIS 6.0 Unsupported Version Detection
2. Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)
3. HP System Management Homepage < 6.0.0.96 / 6.0.0-95
4. HP System Management Homepage < 6.3 Multiple Vulnerabilities
5. HP System Management Homepage < 7.0 Multiple Vulnerabilities
6. HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities
7. HP System Management Homepage < 7.5.4 Multiple Vulnerabilities
8. HP System Management Homepage < 7.6 Multiple Vulnerabilities
9. HP System Management Homepage Multiple Vulnerabilities
10. Microsoft Windows SMBv1 Multiple Vulnerabilities
11. MS09-039: Vulnerabilities in WINS Could Allow Remote Code Executi
12. Unsupported Windows OS (remote)
13. Microsoft Windows Server 2003 Unsupported Installation Detection
14. Microsoft IIS 6.0 Unsupported Version Detection

En estado alto se encuentran:

1. SSL Version 2 and 3 Protocol Detection
2. HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple
3. HP System Management Homepage < 6.2 Multiple Vulnerabilities
4. HP System Management Homepage < 7.1.1 Multiple Vulnerabilities
5. HP System Management Homepage < 7.2.0.14 iprange Parameter
6. HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities
7. HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL
8. HP System Management Homepage < 7.2.6 Multiple Vulnerabilities
9. HP System Management Homepage < 7.6.1 Multiple Vulnerabilities
10. HP System Management Homepage ginkgosnmp.inc Command
11. MS11-035: Vulnerability in WINS Could Allow Remote Code Executio
12. MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote

En estado medio se encuentran:

1. HP System Management Homepage < 7.3 Multiple Vulnerabilities
2. Microsoft Windows SMB LsaQueryInformationPolicy Function SID
3. MS16-047: Security Update for SAM and LSAD Remote Protocols
4. Microsoft Windows SMB NULL Session Authentication
5. SSL Certificate Cannot Be Trusted
6. SSL Medium Strength Cipher Suites Supported (SWEET32)
7. SSL Self-Signed Certificate
8. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerabili
9. Microsoft Windows Remote Desktop Protocol Server
10. Terminal Services Encryption Level is Medium or Low
11. SSL Certificate Signed Using Weak Hashing Algorithm
12. DNS Server Cache Snooping Remote Information Disclosure

Para mayor información ver anexo informe ejecutivo.

Servidor 3 se ejecutó el comando nmap –sP dando como resultado 28 equipos con su respectiva MAC Address, ip y tiempo de conexión o latencia.

Adicionalmente se corrió el comando nmap –p 80 y se detecta que los puertos que se encuentran abiertos son 21, entre los que se encuentra el 389 el cual hace referencia al LDAP
Asimismo, el programa Nessus el cual detecto las siguientes vulnerabilidades sobre los servidores.

6 criticas
1 alta
5 medias
80 informativas

En estado crítica se encuentran:

1. Microsoft Windows SMBv1 Multiple Vulnerabilities
2. MS09-039: Vulnerabilities in WINS Could Allow Remote Code
3. Unsupported Windows OS (remote)
4. Microsoft IIS 6.0 Unsupported Version Detection
5. Conficker Worm Detection (uncredentialed check)
6. Microsoft IIS 6.0 Unsupported Version Detection

En estado alto se encuentran:

1. MS11-035: Vulnerability in WINS Could Allow Remote Code

En estado media se encuentran:

1. Microsoft Windows SMB LsaQueryInformationPolicy Function SID
2. MS16-047: Security Update for SAM and LSAD Remote Protocols
3. SMB Use Host SID to Enumerate Local Users Without Credentials
4. Microsoft Windows SMB NULL Session Authentication
5. DNS Server Cache Snooping Remote Information Disclosure

Para mayor información ver anexo “informe ejecutivo.”

8. Criterios de Seguridad

Otro de los criterios de seguridad que se tuvieron con el análisis de seguridad fue la realización de una matriz que se basó en la norma iso 27001:2013, 27002:2013 de las cuales se tomaron como referencia los siguientes numerales de las normas:

- A.9 Control de accesos
- A.13 Seguridad de las comunicaciones
- A.12.6.1 Gestión de las vulnerabilidades técnicas

y del documento privado de hardering de estandarización para sistemas operativos desarrollado por la compañía ETEK donde se tomaron las configuraciones de los numerales 5.1 criterio política de control de acceso y 5.2 criterio de fortalecimiento y control de red lo cual nos da como resultado el análisis de como se encuentra la entidad en este momento en temas de políticas administrativas y de seguridad bajo las normas mencionadas anteriormente. (Para mayor información ver matriz “matriz de revisión políticas AD”)

9. Recomendaciones

Las amenazas a un sistema de información deben comenzar a tener un papel cada vez mas importante en nuestras prácticas cotidianas, buscando proteger la confidencialidad, la integridad y disponibilidad de la información dicho esto describiremos a continuación algunas recomendaciones que se le pueden dar a la entidad tanto técnicamente como operativamente bajo las normas ISO 27001 y 27002.

Las categorías que se tienen son dos una en el área administrativa o de operación y la otra en el área técnica.

9.1 Recomendaciones en el área administrativa.

- Teniendo en cuenta el numeral A.9 control de acceso con el subnumeral A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.

  Se evidenciaron los siguientes hallazgos la entidad no cuenta con un procedimiento establecido para la autenticación secreta.

  Recomendación: Se recomienda a los dueños de los activos revisar los derechos y privilegios que se tienen de acceso de los usuarios en intervalos teniendo un procedimiento claro para ello.

- Se tomo también el numeral A.9 control de acceso con el subnumeral A.9.2.5 Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.

  Se realizo la verificación en la entidad detectando que no se cuenta con un

procedimiento claro para lograr cumplir con este numeral.

Recomendación: Establecer un proceso claro para que los dueños de los activos logren revisar los permisos que se tienen al ingresar.

- Otro de los numerales que se tomaron fueron el A.9 Control de acceso con el subnumeral A.9.2.6 Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

  Se identifica que la organización no cuenta con un procedimiento para la cancelación de los permisos.

  Recomendación: Establecer un procedimiento claro para que se puedan quitar los permisos a los usuarios tanto internos como externos.

9.2 *Recomendaciones Técnicas*

- Teniendo en cuenta el numeral A.9 con el subnumeral 9.4.3 los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

Historial de contraseñas este control permite mantener un registro de las contraseñas previamente configuradas para su reutilización.

El directorio activo de la entidad cumple con la política de historial de contraseña ya que se tiene el umbral alto que está en el rango de 17 a 24 que es el valor predeterminado que trae el directorio activo.

Recomendación: Se recomienda establecer un procedimiento claro para el historial de

contraseñas ya que no se tiene en este momento en la entidad.

- Edad máxima de contraseña este control permite establecer el tiempo de vigencia de una contraseña, luego del cual esta debe ser modificada.

  El directorio activo de la entidad cuenta con una política de edad mínima de contraseña ya que la que se tiene es de 42 días y no se tiene procedimiento establecido para ello.

  Recomendación: Se recomienda para la edad máxima de contraseña dejar 10 a 15 días hábiles para que se solicite el cambio de contraseña evitando fallos de seguridad en el acceso de usuarios adicionalmente se sugiere establecer un procedimiento para ello.

- Requiere llave de encripción fuerte este control permite indicar que se utilice llaves de sesión de 128-bit para la comunicación a través de un canal seguro hacia el controlador de dominio y otras estaciones o servidores que se encuentren en el dominio.

  La entidad no cumple con la política de llave de encriptación fuerte ya que en este momento se encuentra deshabilitada esta política y no se tiene un procedimiento establecido para asegurar la contraseña de usuario.

  Recomendación: Se recomienda habilitar la política de encripción fuerte para que las comunicaciones que van hacia el controlador de dominio sean autenticadas y evita posibles accesos indebidos también se encomienda tener el procedimiento de la política de contraseña segura ya que no se tiene en este momento.

- Envío de Password no cifrados a servidores smb este control ayuda a prevenir que la información de inicio de sesión que incluye credenciales pueda ser interceptada por usuarios maliciosos.

La entidad no cumple con la política de envió de Password no cifrado a los servidores smb ya que en el directorio activo se encuentra en la opción “Enable” o habilitada.

Recomendación: Se recomienda tener la política deshabilitada la opción cliente de redes de Microsoft enviar contraseña no cifrada para conectarse a servidores SMB de terceros. Ya que si habilita esta configuración de Directiva, el servidor puede transmitir contraseñas de texto sin formato a través de la red a otros equipos que ofrezcan servicios SMB. Es posible que estos otros dispositivos no usen ninguno de los mecanismos de seguridad de SMB que se incluyen en Windows Server2003 o versiones posteriores también se sugiere tener un procedimiento para esto.

- Nivel de validación que desarrolla una comunicación al servidor SPN este control permite controlar el nivel de validación que un computador con directorios compartidos o impresoras o servidores, que desarrolla con el servidor SPN (nombre principal de servicio) mediante el protocolo SMB (server message block), evitando vectores de ataques como SMB relay evitando la suplantación de la identidad de un computador para ganar acceso no autorizado a los recursos en la red

  La entidad no cumple con la política de nivel de validación que se desarrolla con la comunicación al servidor SPN ya que este momento no se encuentra habilitada esta política.

  Recomendación: Se recomienda habilitar esta opción en el directorio activo ya que esta configuración de directiva controla el nivel de validación que un servidor con carpetas o impresoras compartidas realiza en el nombre principal de servicio (SPN) proporcionado por el dispositivo cliente cuando el dispositivo cliente establece una sesión con el protocolo SMB. El nivel de validación puede ayudar a evitar una clase de ataques contra los servidores SMB (denominados ataques de retransmisión SMB). Esta configuración afectará a SMB1 y SMB2.

- La norma ISO 27001 y 27002 en su numeral A.12. SEGURIDAD DE LAS OPERACIONES. y el subnumeral A.12.6.1. define “Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado”

  Mantener los servidores y sistemas de información donde se encuentra el directorio activo actualizado.
  La entidad no cumple con esta política ya que los sistemas con los que cuenta son obsoletos y en algunos casos no se encuentran actualizados.

  Recomendación: Se recomienda realizar un escaneo de vulnerabilidades logrando mitigar al mínimo los riesgos reportado por las diferentes herramientas que existen en el mercado también se recomienda instalar las actualizaciones Microsoft ya que no se tienen todos los Service pack instalados.

10 Prueba Piloto de remediación de vulnerabilidades del controlador de dominio veeduriadistrital2.gov.co

Teniendo en cuenta el numeral A.12. SEGURIDAD DE LAS OPERACIONES. y el subnumeral A.12.6.1. que define “Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado”, se procedió a realizar el pilotaje de análisis de vulnerabilidades en un entorno controlado que describimos a continuación:

Después de realizar la virtualización del servidor VD-SERVER2 único servidor del dominio veeduriadistrital2.gov.co se procedió a configurar la imagen en la plataforma virtual

vmware versión 12 se comprobó conectividad y se realizó escaneo con la herramienta nmap encontrándose 32 puertos abiertos.

Después se realizó el escaneo de vulnerabilidades inicial con la aplicación nessus profesional donde se obtuvieron los siguientes resultados de vulnerabilidades:

Criticas	Altas	Medias	Bajas
48	511	113	11

Se observo que al realizar el escaneo de vulnerabilidades en el entorno controlado con conexión directa al host de virtualización vario la cantidad de vulnerabilidades encontradas así:

	Criticas	Altas	Medias	Bajas
Análisis realizado en la entidad	13	12	14	2
Análisis en entorno controlado	48	511	113	11

Se verifico y del año 2010 a la fecha de escaneo solo se tenían 2 actualizaciones del 24/07/2012 y una del 19/05/2017, se procedió a realizar a descargas e instalar las actualizaciones del sistema donde se encontraron 157 actualizaciones.

Después de realizar la instalación se generó un nuevo escaneo de vulnerabilidades con la herramienta nessus arrojando la siguiente información:

Criticas	Altas	Medias	Bajas
37	284	68	9

Se verificaron las actualizaciones y se realizaron algunas de las remediaciones indicadas de Adobe y hp Management después se generó un nuevo reporte de vulnerabilidades generando el siguiente reporte:

Criticas	Altas	Medias	Bajas
31	268	65	7

Se remediaron algunas actualizaciones de mozilla y se generó nuevamente el escaneo de

vulnerabilidades obteniendo los siguientes resultados:

Criticas	Altas	Medias	Bajas
28	203	55	6

Se corrigieron algunas vulnerabilidades desde el registro de Windows y se generó nuevamente el escaneo de vulnerabilidades obteniendo el siguiente resultado:

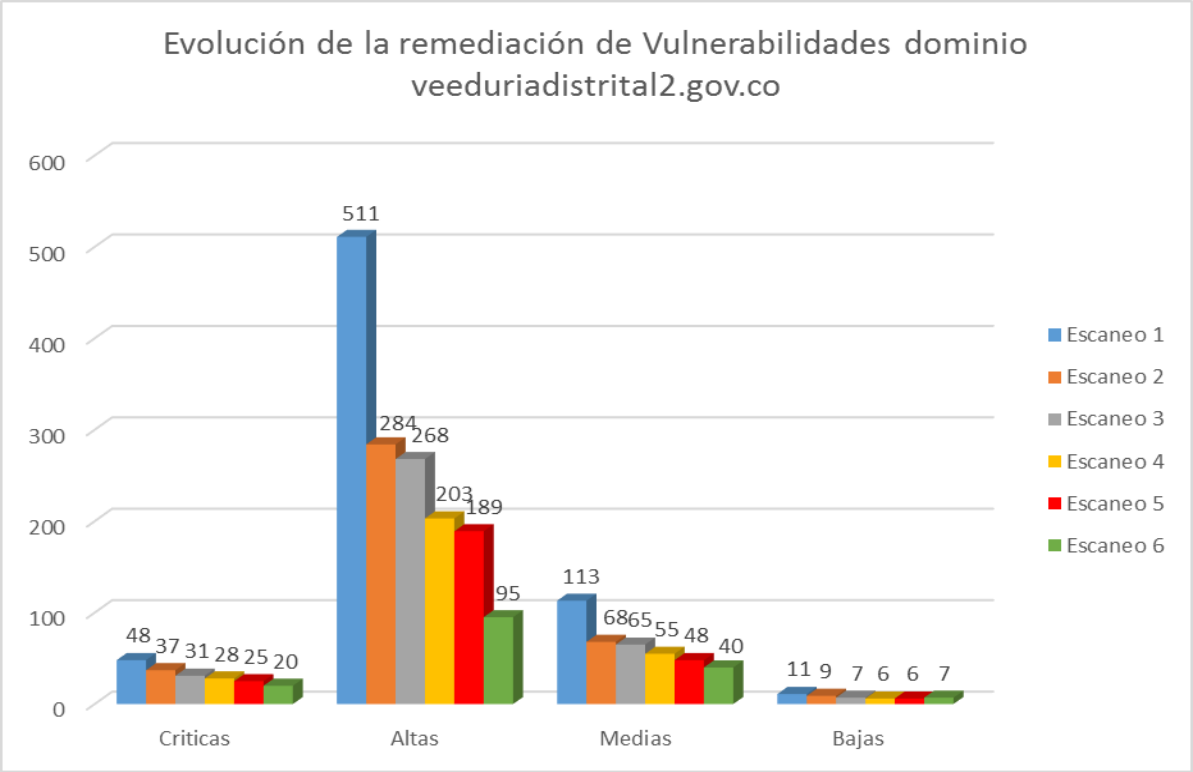
Criticas	Altas	Medias	Bajas
25	189	48	6

Por último, se corrigieron algunas vulnerabilidades asociadas a versiones desactualizadas de .net framework y se generó nuevamente el análisis de vulnerabilidades

Criticas	Altas	Medias	Bajas
20	95	40	7

Conclusión:

Después de realizar algunas de las remediaciones indicadas en los análisis de vulnerabilidades se observó una disminución considerable como se muestra en la siguiente gráfica:



Fuente Fabio Franco Imagen 5

Se actualizaron las diferentes versiones de adobe (acrobat reader y flash player), mozila, internet explorer, hp management a las últimas versiones del sistema operativo Windows 2003 Server SP2 pero continuaban apareciendo las vulnerabilidades indicando que se requería actualizar el sistema operativo ya que las últimas versiones de los aplicativos no eran soportadas por el sistemas operativo instalado, este sistemas salió de soporte el 14 de julio de 2015.

Teniendo en cuenta que todos los servidores que soportan los 3 dominios de la entidad están sobre el sistema operativo Windows 2003 Server SP2 producto que se encuentra fuera de soporte por el fabricante recomendamos actualizar a un sistema operativo soportado para que puedan ser parchados el sistema operativo y los aplicativos instalados sobre cada uno de los servidores.

La información de los resultados de los análisis puede ser consultada en el anexo “remediación de vulnerabilidades”.

11 CONCLUSIONES

El presente trabajo de grado tuvo como objetivo realizar un análisis de vulnerabilidades a los diferentes servidores de directorio activo de la veeduría distrital donde validamos el estado actual, los autores compararon algunos de los requerimientos de la norma ISO 27001:2013 en los temas de control de acceso, seguridad de las comunicaciones y gestión de las vulnerabilidades técnicas de los donde generamos las recomendaciones incluidas en el presente documento, como resultado los autores generaron las siguientes las siguientes conclusiones:

En la evaluación realizada a las configuraciones de control de acceso desde el directorio activo no encontraron una adecuada configuración en cuanto a los temas de manejo de contraseñas como son complejidad, caducidad, reúso, longitud, etc, lo que puede llevar a la entidad a presentar debilidades de seguridad si un usuario experto accede a la entidad pudiendo afectar la integridad, disponibilidad y confidencialidad de la información.

Cuando los autores realizaron en escaneo de vulnerabilidades al interior de la entidad vs el análisis que realizaron en el entorno controlado observaron un aumento significativo de vulnerabilidades ya que la entidad tiene una adecuada configuración a nivel de permisos de red entre los diferentes segmentos, no obstante, las vulnerabilidades encontradas desde la red de la entidad pueden llegar a ser explotadas por un usuario experto para afectar a la entidad.

En la evaluación que los autores realizaron a la documentación de la entidad en cuanto a creación de usuarios y perfilamiento encontraron que están definidos correctamente los niveles de aprobación y el proceso a realizar por los responsables, en la evaluación documental a los procedimientos de gestión de vulnerabilidades no encontraron nada relacionado por lo que sugieren crear los procedimientos para fortalecer a la entidad en cuanto a la oportuna detección e implementación de soluciones de remediación de vulnerabilidades en los diferentes componentes tecnológicos con los que cuenta.

Cuando los autores realizaron el levantamiento inicial de la configuración del directorio

activo encontraron que se tienen creados 3 dominios lo cual es poco funcional y genera una carga alta operativa ya que en todos se tiene usuario y equipos vinculados.

De acuerdo con los resultados obtenidos en el piloto de solución de vulnerabilidades realizado por los autores se concluye que los sistemas operativos Windows 2003 Server de los servidores analizados están obsoletos desde el 14 de julio de 2015 por lo que en el piloto no se pudo afinar completamente el servidor y disminuir a 0 las vulnerabilidades críticas y altas encontradas.

Teniendo en cuenta la evaluación realizada por los autores y los resultados obtenidos concluyen que la entidad en los puntos evaluados tiene un nivel bajo de seguridad que un usuario experto puede llegar a explotar para afectar la integridad, disponibilidad y confidencialidad de la información de la entidad.

12 BIBLIOGRAFÍA

Servicios de dominio del directorio activo consultada 22-08-2019

http://www.ticarte.com/sites/su/users/7/arch/que_es_el_directorio_activo_dominios_arboles_y_bosques.pdf

Guía de Planeación y diseños de AD DS Microsoft 06-08-2018 consultada 17-09-2019

https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/ad-ds-design-and-planning

Guía de procedimiento Microsoft recomendada para proteger el Active Directory Microsoft 30-05-2017

https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Guía Microsoft para la protección de los controladores de dominio frente a ataques fecha 17-06-2017

https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack

Guía reducción de la superficie de ataque de Directory active Microsoft 30-05-2017

https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/reducing-the-active-directory-attack-surface

Detección de abuso de privilegios de administrador de dominio mediante el Registro de eventos de Windows 21-11-2018

https://www-scopus-com.ucatolica.basesdedatosezproxy.com/record/display.uri?eid=2-s2.0-85062852500&origin=resultslist&sort=plf-f&src=s&st1=directory+active&st2=&sid=bd23d02528040f04d19465abf24547ee&sot=b&sdt=b&sl=31&s=TITLE-ABS-KEY%28directory+active%29&relpos=8&citeCnt=0&searchTerm=#references

Active Directory y aspectos relacionados de seguridad 25-04-2018

https://www-scopus-com.ucatolica.basesdedatosezproxy.com/record/display.uri?eid=2-s2.0-85061512435&origin=resultslist&sort=plf-f&src=s&st1=+vulnerabilities+in+the+active+directory&st2=&sid=bd23d02528040f04d19465abf24547ee&sot=b&sdt=b&sl=55&s=TITLE-ABS-KEY%28+vulnerabilities+in+the+active+directory%29&relpos=1&citeCnt=0&searchTerm=#references

Boletín de seguridad Microsoft MS07-039 critica 10-10-2017

https://docs.microsoft.com/es-es/security-updates/securitybulletins/2007/ms07-039

Detalle de vulnerabilidad CVE-2011-3406 fecha 10-30-2108

https://www.cvedetails.com/cve/CVE-2011-3406/

Mejores prácticas para asegurar el directorio activo Microsoft 30-05-2017

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

13 ANEXOS

13.1 INFORME EJECUTIVO DEL ANÁLISIS

Informe Ejecutivo 13.1.docx

13.2 Matriz de Criterios de seguridad

matriz de revision politicas AD.xls

13.3 Remediación de Vulnerabilidades

13.3 Remediación de Vulnerabilidades.doc